REMARKS:

Claims 105-107, 109-118 and 127-167 remain pending in the application. Claim 132 has been amended to insert the word "the." Applicant respectfully requests entry of this amendment.

Claim 105

The Examiner uses Kouznetsov as the basis for the pending obviousness rejection of claim 105. Yet Kouznetsov takes a fundamentally different approach to achieving "security of [a] computer system." In Kouznetsov, "[s]uspsect sequences of potentially viral activity are identified and histograms are generated." Kouznetsov at 2:38-39. Kouznetsov continues: "A virus alert is generated if the histograms illustrate repeated suspect sequences." Accordingly, Kouznetsov's security paradigm is based on the identification of "[s]uspect sequences." *Id.* at 2:39-40. The Examiner concedes that "Koutnetsov does not explicitly disclose a weighing functionality that scores/determines the monitored events/code under investigation as valid/non-malicious code." *See* Office Action 3.[1] The Examiner attempts to remedy this deficiency using Chess and Hill.

Applicant does not understand the Examiner's explanation of how Chess and Hill would be used to modify Kouznetsov to achieve the combination recited in claim 105. Kouznetsov, Chess, and Hill exploit very different security paradigms. Thus, even assuming these references could be combined, it is not clear what such a combination would look like. Is the Examiner suggesting that Kouznetsov's "collector" trigger on "non-suspect" behavior as well? If so, Applicant fails to see where such a suggestion comes from, as Chess merely teaches the determination of a *file* as malicious or non-malicious. Even more problematic, however, is that a behavior analyzer that triggers on both suspect *and* non-suspect behavior would not seem to make sense to one of ordinary skill in the art, at least for performance reasons. However, leaving aside the issue of how Kouznetsov and Chess are to be combined, Applicant submits that even if

[1] Applicant respectfully submits that Kouznetsov does not teach or suggest several other features of claim 105 as well. First, it is not clear that Kouznetsov's static and dynamic analyzers correspond to either of the "first" and "second" "plurality of detection routines." Second, Applicant strongly disagrees that Kouznetsov's "histogram" corresponds to "weighting *each* of the second *plurality* of results to obtain a second score." Applicant respectfully submits that the Examiner's analysis does not take into account each word in claim 105.

Chess were combined with Kouznetsov, Chess does not teach or suggest "weighting," much less "weighting" a "*plurality* of results" as recited in claim 105. Furthermore, the combination of Kouznetsov and Chess does not teach or suggest "using the first *and* second scores to categorize the code under investigation…." Kouznetsov is only interested in "suspect" activity, and neither Kouznetsov nor Chess teaches or suggests "scores" as recite in claim 105.

The Examiner apparently relies on Hill to teach the "score" recited in claim 105. Applicant submits that Hill's "attack severity 61" is not computed in the manner described for the recited "first" and "second" "scores." Furthermore, Hill's attack severity 61 corresponds to a "security attack 92." This security attack is thus not "code under investigation" that has not yet b been "categorize[d]," but rather corresponds to a known security threat. At a minimum, then, attack severity 61 (or any value pointed to by the Examiner in Hill) cannot and does not correspond to the "first score" of claim 105. Yet again, the present Office Action does not adequately explain how Hill is to be combined with Kouznetsov and Chess, and why it is even relevant.

For at least the reasons stated above, Applicant submits that claim 105 (and, by extension, its dependent claims) are in condition for allowance.

As a further note, Applicant would like to direct the Examiner's attention to an Office Action issued in U.S. Appl. No. 10/231,557 (the parent application to the present application) dated October 30, 2007. In that Office Action, the Examiner rejected a number of pending claims of the '557 application based on Muttik (specifically column 4, line 59 to column 5, line 17) [2] and Dozortsev. In a response dated January 30, 2008, Applicant argued this rejection, noting that Muttik's "count of the total weight" did not teach or suggest the "first" and "second" "composite scores" of the pending claims in the '557 application.

Claim 106

Dependent claim 106 recites "wherein execution of the MCDC does not preclude the selected active code from *directly interfacing with an operating system* of the computer system." **The Examiner does not even address this language in the present Office Action.** *See* Office

[2] Applicant notes that Muttik (U.S. Patent No. 6,775,780) is already of record in this application.

Action at 4 (addressing only a portion of the language of claim 106). As such, the Examiner has failed to establish a *prima facie* case of obviousness with respect to claim 106.

This omission is not insignificant, as Kouznetsov describes "monitor/analyzer 10" as "a logical 'shim' *interposed between the operating system 32 and each of the applications 33, 34, and 35*" and that "intercept[s] system call[s]." Kouznetsov, 4:18-20. Accordingly, the additional features recited in claim 106 are not taught or suggested in Kouznetsov, and it does not appear that the Examiner contends such features are found in Chess or Hill. Applicant further submits that to modify Kouznetsov to change the analyzer's status as a "logical 'shim'" would render Kouznetsov interoperable for its intended purpose, as it would no longer be able to "intercept[]" and "analyze" system calls. As such, Applicant submits that Kouznetsov is not modifiable to teach or suggest the limitations of claim 106. For at least these additional reasons, claim 106 is believed to be further patentably distinct over the cited references.

Claim 107

The Examiner alleges that Kouznetsov's monitoring of incoming system calls corresponds to claim 107's "selecting, in turn, *each* additional active program on the computer system." Applicant submits that these limitations are not inherent in Kouznetsov, and that Kouznetsov, does not, "in turn" select[]" an "active program" and then "execute[] said MCDC with respect to said selected code…" For at least these additional reasons, claim 107 is believed to be further patentably distinct over the cited references.

Claim 115

The Examiner alleges that Kouznetsov teaches "selecting code" that is "running in a manner that permits infection of said computer system." *See* Office Action at 4 (rejecting claim 115 on the same basis as 105, although not specifically addressing the additional language). Applicant submits that it is not clear that Kouznetsov's "logical 'shim'" "permits infection of said computer system." For at least these additional reasons, claim 115 and its dependent claims are believed to be further patentably distinct over the cited references.

Claims 117 and 151

Claim 117 recites "wherein at least some of the code associated with the selected active code is running in kernel mode." The Examiner rejects this claim on the same basis as claim 115, but does not appear to further address this limitation. Accordingly, Applicant submits that the Examiner has not made a *prima facie* case of obviousness with respect to claim 117, and submits that for at least this additional reason, claim 117 is further patentably distinct over the cited references. Claim 151 is believed to further distinguish over the cited references for at least the reasons provided in support of claim 117.

Claims 127 and 128

These claims and their respective dependent claims are believed to be patentably distinct over the cited references for at least the reasons provided for claims 105 and 115.

Claim 131

Dependent claim 131 recites that the "first plurality of detection routines includes routines that examine the *behavior* of the code under investigation." Note that claim 105, from which claim 131 depends, recites that the "first plurality of detection routines" are "indicative of whether the code under investigation has characteristics and/or behaviors typically associated with *valid* code." At best, Kouznetsov teaches only examining "suspect" behavior. *See* discussion of claim 105, *supra*. Chess does not teach examining behavior at all. Hill deals with measuring attack severity. Thus, none of the cited references teach that the "first plurality of detection routines includes routines that examine the behavior of the code under investigation." For at least this additional reason, claim 131 and its dependent claim 132 are believed to be patentably distinct over the cited references.

Claims 137

Claim 137 recites "determining from the first and second scores that the code under investigation is suspicious code, wherein suspicious code has not been determined to be either valid or malicious code." Applicant notes that in the context of the present application, "suspicious" code is different from "malicious" code or "valid" code. *See* paragraph [0047] of

the published version of this application. Further, claim 137 defines "suspicious code" as that code which "has not been determined to be either valid or malicious code." Note that claim 137 recites "*determining*" that "the code under investigation *is* suspicious code." Thus, within claim 137, code is not first deemed "suspicious" *before* "determining"; rather, the "determining" *results in* "code under investigation" being deemed "suspicious." For at least these reasons, then claims 137 and 138 are believed to be patentably distinct over the cited references. Claims 144, 149, 157, and 158 are believed to be patentably distinct for at least reasons similar to those provided for claim 137.

Claim 167

Claim 167 is believed to be patentably distinct over the cited references for at least the reasons provided for claim 105. Additionally, the Examiner is not believed to have provided the proper analysis with respect to a claim with means-plus-function limitations. *See* MPEP § 2181, *et seq.*

CONCLUSION:

Applicants submit the application is in condition for allowance, and an early notice to that effect is requested.

If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above-referenced application from becoming abandoned, Applicant hereby petitions for such extension.

The Commissioner is authorized to charge any fees that may be required, or credit any overpayment, to Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C. Deposit Account No. 501505/6002-00602/DMM.

Respectfully submitted,

Date: February 11, 2008

By: /Dean M. Munyon/
Dean M. Munyon
Reg. No. 42,914

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P. O. Box 398
Austin, Texas 78767
(512) 853-8847